Publisher Universal CloudSaaS Additional Terms and Conditions

Federal Risk and Authorization Management Program (FEDRAMP) and DoD Cloud Computing (CC) Security Requirements Guide (SRG) REQUIREMENTS.
The Publisher's products are hosted by Amazon Web Services or Amazon Web Services GovCloud which is FEDRAMP certified. Publisher certifies it has implemented the security controls in the applicable System Security Plan.

Publisher shall, at a minimum, maintain the security controls described in the System Security Plan.

Section 2. DOD Cloud Requirements

a. All service sites and disaster recovery sites (DR) will be performed CONUS and all associated support services (eg. help-desk) will also be CONUS.

b. Publisher will report to DoD any and all data breaches (as defined by CC SRG 6.5.1 involving DoD data or Personally Identifiable Information (PII) of Authorized Users. Publisher must report such data breaches in accordance with Publisher's Incidence Response Plan. The report must include, to the extent the following information is known by Publisher, the date, time, location and possible scope of the breach, the nature of the data compromised if known, the means of breach, the date, time and means of discovery of the breach, immediate remediation steps taken and longer term remediation steps taken. In no event will Publisher delay reporting a breach if all of the outlined factors listed above are not fully known. DoD retains all rights and remedies at law and in equity for data breaches, including but not limited to appropriate remediation of transactional or PII information. To the extent Publisher, or a 3rd party engaged by Publisher to deliver the Services is at fault, PII remediation provided by Publisher at Publisher's sole cost and expense will include identity theft remediation for each Authorized User whose PII was breached for a period of one year after the breach.

Section 3. **Performance Metrics.** In accordance with the CC SRG, Publisher will,

a. Perform, and disclose within the U.S. Government, any benchmark or performance tests of the services, including the Publisher programs;

b. Perform and disclose within the U.S. Government, security testing of the services environments or associated infrastructure, including any of the following: network discovery, port and service identification, vulnerability scanning, password complexity, remote access testing, or penetration testing.

Section 4. **Technology Professional Liability Errors and Omissions Insurance.** Publisher shall maintain Technology Professional Liability Errors and Omissions Insurance, with limits not less $4,000,000 in the annual aggregate.

a. Coverage shall include, but not be limited to, data breach, invasion of privacy violations, information theft, release of private information, extortion and network security unauthorized access and use, failure of security, breach of confidential information, of privacy perils, as well as breach mitigation costs and regulatory coverage

b. Such insurance shall also provide coverage for, among other things, damage to, alteration of, loss of, or destruction of electronic data and/or information "property" of the DOD that will be in the care, custody,

or control of Publisher and provide coverage for breach response costs as well as regulatory fines and penalties as well as credit monitoring expenses.

c. No representation is made that the minimum Insurance requirements of this agreement are sufficient to cover the indemnity or other obligations of the Vendor under this agreement.

d. Such insurance shall be maintained in force at all times during the term of the agreement and for a period of two years thereafter for services completed during the term of the agreement. The DOD shall be given at least 30 days notice of the cancellation or non-renewal of the aforementioned insurance for any reason.